Report (/)

Weekly Threat Report 29th September 2017

Created: 29 Sep 2017
Updated: 29 Sep 2017

We would like your feedback on the Weekly Threat Report. Please send us your thoughts, suggestions and queries using our 'Contact Us(/contact)' page.

This report is drawn from recent open source reporting.

Compromise of Deloitte

The Guardian this week reported that the global accountancy firm Deloitte had been hit by a cyber attack that has revealed client email addresses. The hackers may have also accessed usernames, passwords and personal details.

Deloitte provides auditing, tax consultancy and cyber security advice to some of the world's biggest banks, multi-national companies, media enterprises, pharmaceutical firms and US government agencies. According to the Guardian, Deloitte clients across these sectors had material in the company email system that was breached. The breach was believed to be US-focussed, affecting well-known companies as well as US Government departments. The compromise was discovered in March this year, but it was reported that the attackers may have had access to Deloitte systems since October or November 2016.

According to the newspaper, the hacker compromised the firm's Microsoft Azure Cloud global email server through an administrator's account that, in theory, provided them with privileged, unrestricted access. The account required only a single password and did not have "two-step" verification. Emails to and from Deloitte's 244,000 staff were stored in the Azure cloud service which is Microsoft's equivalent to Amazon Web Service and Google's Cloud Platform.

Deloitte has stated on its website that only very few clients were impacted and no disruption has occurred to client businesses, to Deloitte's ability to serve clients, or to consumers. The NCSC statement(/news/statement-deloitte-cyber-incident) confirmed that we had engaged with the organisation to better understand the threat and based on current information we understand there to have been minimal UK impact.

Using a single factor authentication system like a username and an easy-to-guess password combination has allowed criminals to gain access to a user's account. Simple passwords based on dictionaries or the same passwords used on other systems that may have been leaked can give cyber attackers easy access to IT systems. Gaining access to the administrator account is the 'jackpot' for an attacker and will provide an attacker with unrestricted access to all user accounts.

Two Factor Authentication (or 2FA) is an extra layer of security that requires not only a password and username but also something that only that user has on them, i.e. a piece of information only they should know or have immediately to hand - such as a physical token, keyfob device, fingerprint, facial recognition or SMS confirmation via mobile phone.

A compromise would be highly unlikely if a complex password or 2FA had been implemented. See the NCSC's Password Guidance(/guidance/password-guidance-simplifying-your-approach).

Banks' concerns about cloud cyber security

Investment bank Goldman Sachs has in recent days echoed concerns about the number of banks using the same small number of Cloud storage providers – pointing out that those users also include the UK financial regulatory bodies.

The bank's Head of Technology for Europe, Middle East and Africa argues that the online platforms should be regulated from a resilience perspective, and describes a 'concentration risk'. The concerns echo those voiced in January by the Bank of England Governor and the chair of the Financial Stability Board, who refer to the risk of a single point of failure if 'banks come to rely on common hosts of online banking or providers of Cloud computing services'.

The use of an online network, or 'Cloud', increases the scale and flexibility of computing capacity, and aligns with the growing desire within the financial services industry for innovative technological business models and processes.

The Financial Stability Board (FSB) alerted the industry in June to the greater reliance on external providers of technology, and hence the potential risk of disruption, specifically citing the Cloud. The FSB highlighted the risks of financial institutions relying on the same third-party Cloud computing and data services providers, and cited other jurisdictions where, for example, guidelines had been issued for Cloud outsourcing, internet banking and technology risk management. Greater co-ordination within finance, and with non-finance partner organisations such as those with a remit for cyber security, was mooted.

Some of the growing concerns voiced within financial services about the Cloud are addressed by the NCSC's Cloud Security Principles and advice(/topics/cloud-security).

Cryptocurrency mining by cyber criminals

Recent IBM reporting observes a sixfold increase in the use of specifically CPU-based cryptocurrency-mining malware since the beginning of 2017, a much faster rise than observed for cryptocurrency-mining malware more generally.

While there are many cryptocurrencies, with different characteristics, all rely on 'miners', who carry out large number of calculations to verify transactions. In exchange for contributing computing power, miners are rewarded with cryptocurrency.

Mining many currencies using a CPU has generally become economically unviable for legitimate users, as running costs outweigh their gains, so they now use graphics cards, or specially designed application-specific integrated circuits (ASICs). Running costs are no obstacle to cyber criminals, however, who can use botnets of compromised machines as miners without needing to worry about the electricity bills. Some newer currencies are also more feasible to mine using a CPU only.

In a related trend, an increasing number of website scripts are being observed which mine cryptocurrency inside a web browser. Such scripts can be used in clearly illegal ways when hidden within adverts (a form of malvertising), but some sites have also shown an interest in such scripts as a form of revenue production to replace or supplement online advertising. Torrenting site The Pirate Bay received significant press coverage when it was revealed to have adopted such scripts without the knowledge or consent of its users. There have also been reports of cyber criminals compromising popular websites and hiding mining scripts in their source code, allowing them to profit from their victim's visitors.

--

The Cyber Security Information Sharing Partnership (CiSP) is a great way of learning more about threat information as well as engaging with industry and government counterparts. Follow the link below for more information.

Join CiSP(/cisp)

Topics

Cyber threats(/topics/cyber-threats)
Cyber attacks(/topics/cyber-attacks)
Vulnerabilities(/topics/vulnerabilities)

Was this report helpful?

We need your feedback to improve this content.

Yes No